www.markany.com

Data Loss Prevention(DLP)

SafePC Enterprise v 7.0

Build a Safer World, Protect What Matters.

MarkAny

SafePC Enterprise (DLP)

Contents

MarkAny

DLP(Data Loss Prevention)

DLP stands for Data Loss Prevention, which means data loss protection.
It protects your organization's internal data from being compromised by blocking the pathways through which it can leak from your PC to the outside.
It provides policies to detect sensitive information (personal information) on PCs and control the devices, networks, and prints.

Protecting enterprise data

Enhance data security by detecting and blocking the leakage of confidential or private information within your business or organization to the outside.

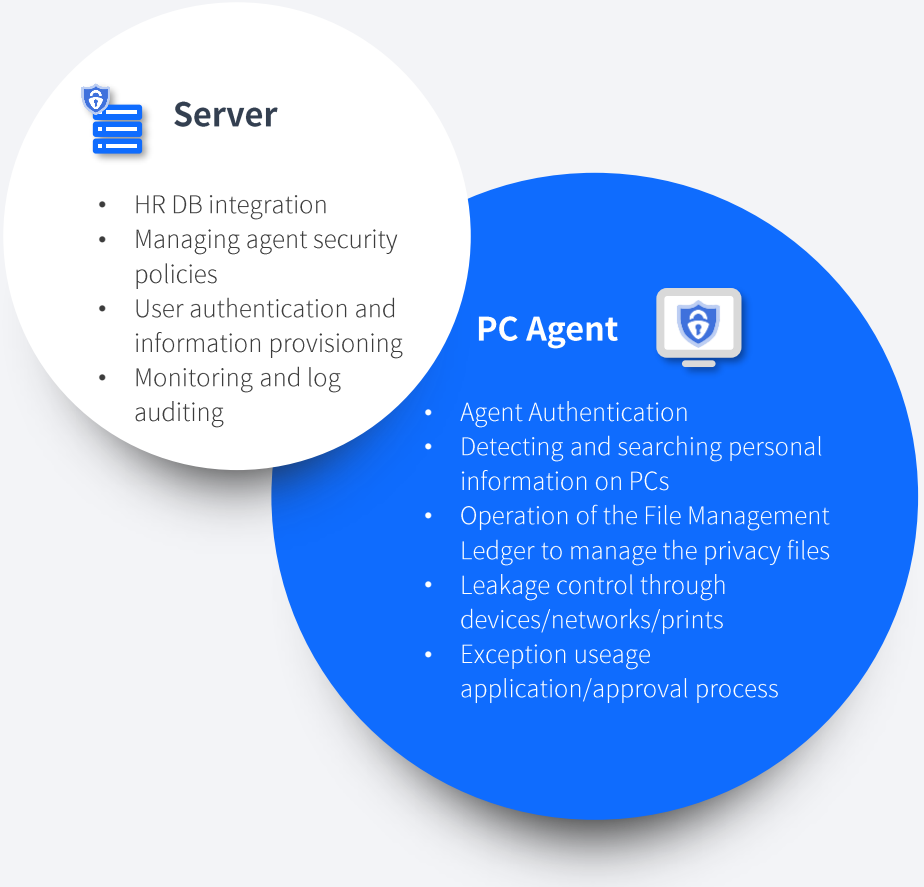
Compliance with laws and regulations

By adopting a DLP, you can comply with various IT compliance such as the Information and Communications Network Act and the Personal Information Protection Act.

Rapid response

It provides a variety of audit logs and monitoring to help you quickly detect and respond to data breaches.

II . DLP Configurations



Supported OS

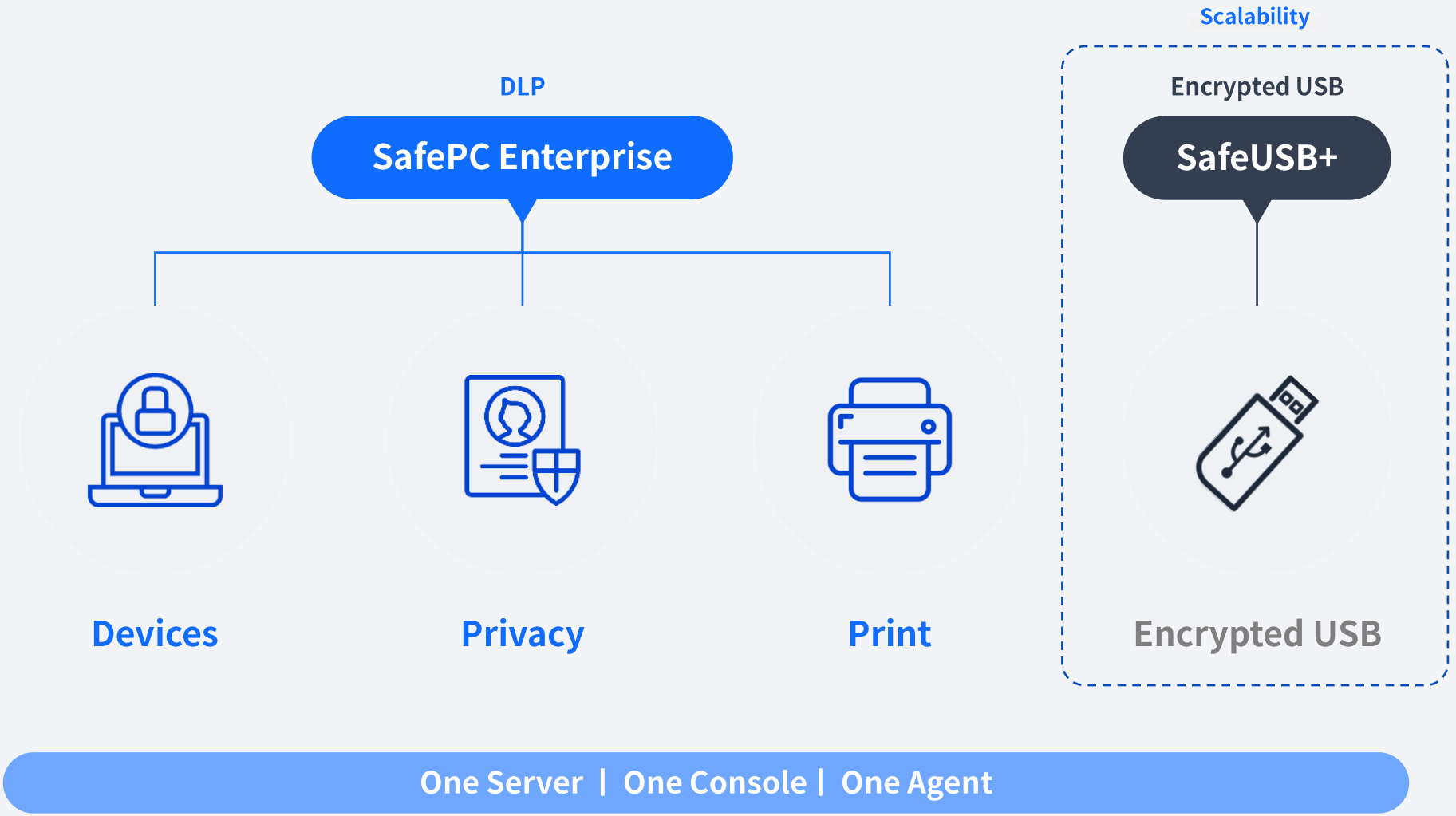
- Server : Redhat 8 / Maria DB 10
- PC Agent : Windows 10, 11

Centralized management

- Administrators can create and enforce policies, view audit logs, and monitor using the web console

HR DB Integration

- Establish company, department, and individual user policies after linking department and user information for flexible operation



SafePC Enterprise V7.0

DLP(Data Loss Prevention)

DLP stands for Data Loss Prevention, which means data loss prevention.
It detects sensitive information (personal information) within a PC and controls it from leaking to the outside through devices, networks, prints.
SafePC Enterprise is Endpoint DLP, where controls are performed by PC Agent.

Device

- Device controls
  (auxiliary storage and data transfer devices)
- Online controls
  (website access blocking, firewalls, etc.)
- Program execution control
- Control of other PC settings

Privacy

- Scan (index) all documents on PCs to identify whether they contain privacy based on patterns
- Block leakage when privacy is included(Storage, online, printout, shared folders, etc.)
- Manage personal information using the File Management Ledger

Print

- Printing Allow/Block policies
- Insert image, text watermarks
- Insert publisher information
- Controlling the print and masking personal information in the printout

III. Main Features – Overview

MarkAny

Device Control

- Allow (Read/Write) / Block Storage devices
- Allow / Block Data transfer devices
- General storage devices (USB, external HDD, etc.) registration management

Privacy

- Detect personal information based on regular expressions, keyword patterns
- Leakage control through devices, networks, and printouts

Network Control

- Controlling website access
- File Attachment Control (File Size)
- Personal Firewall

File Management Ledger

- Manage the registration of detected privacy files
- Provide settings such as registration grace period, expiration warning period, retention period, etc.
- Encryption/complete deletion/ notification of files containing personal information

PC Security Setting

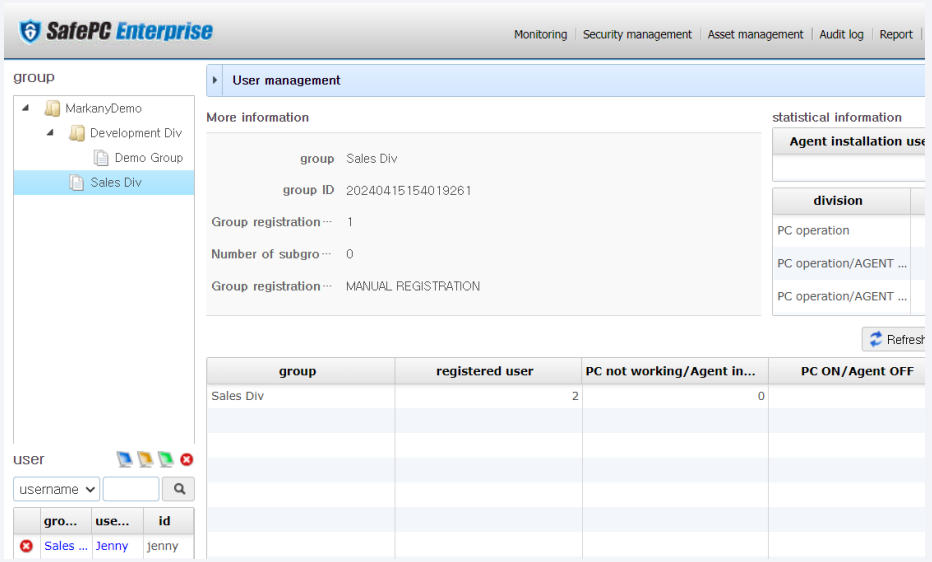
- Control shared folders (block creation and unshare)
- Screensavers (force and timed)
- Block programs from running

Print Control

- Allow/Block printing policies
- Insert image, text watermarks
- Insert publisher information
- Controlling the print and masking personal information in the printout

III. Main Features – User Authentication

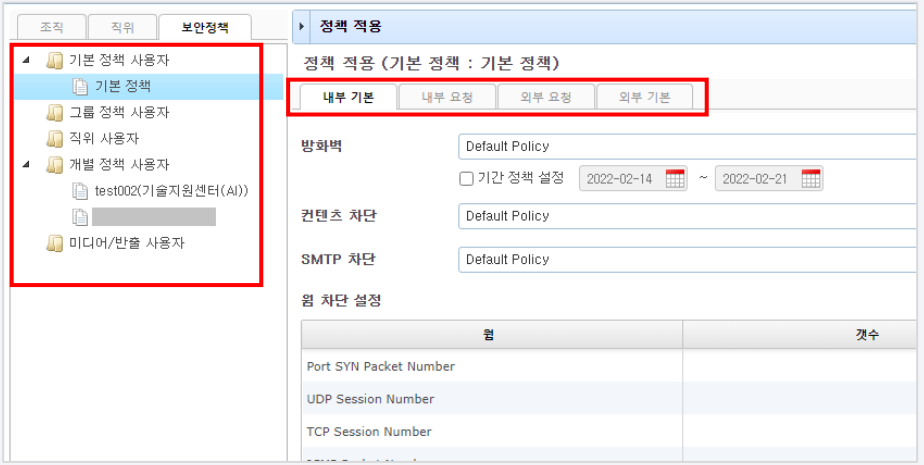
[Log in to the Agent]



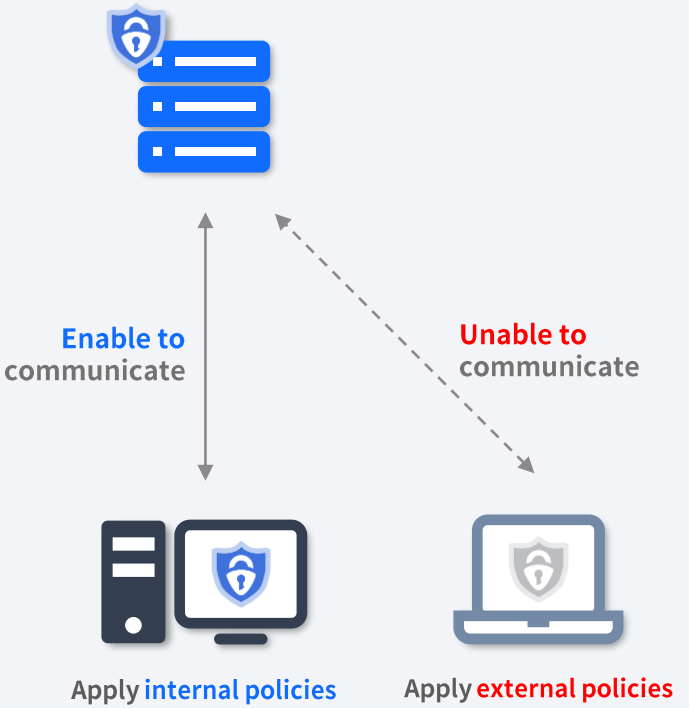
[User management]

- Link and manage department and user information
- After installation, users are authenticated with an ID/authentication code, and enter a password based on password generation rules
- On subsequent boots, enter the password of the authenticated account to log in

III. Main Features – Centralized policy management



[Apply policies]

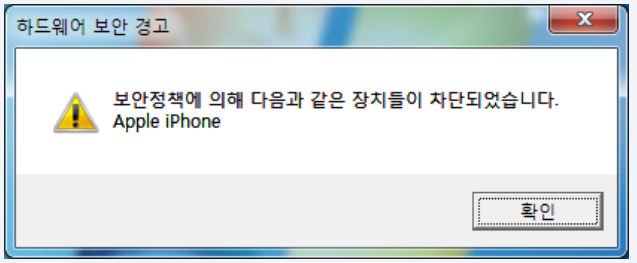


- Internal/external policies can be applied (internal/external with/without server communication, respectively)
- Priority of policies is applied in the order of Media/Export > Individual > Position > Group > Default (All)
- Policies approved using the approval process are applied as policies on the Request tab

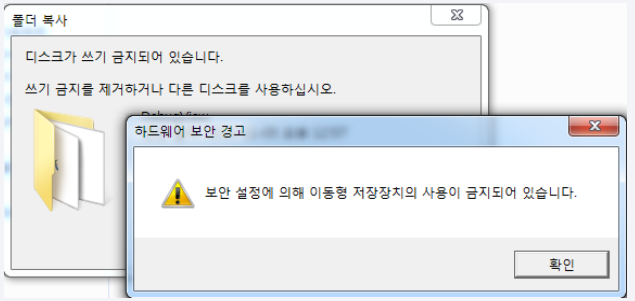
III. Main Features – Device Control

Media name	current permissions	Apply for permission
Floppy disk	Write block / Block reading	☐ Allow writing / ☐ Allow reading
CD/DVD	Write block / Block reading	☐ Allow writing / ☐ Allow reading
PDA	Write block	☐ Allow writing
Infrared port	Write block	☐ Allow writing
Serial port	Write block	☐ Allow writing
Storage device	Write block / Block reading	☐ Allow writing / ☐ Allow reading
Parallel port	Write block	☐ Allow writing
Wireless LAN	Write block	☐ Allow writing
Bluetooth	Write block	☐ Allow writing
HSDPA	Write block	☐ Allow writing
WIBRO	Write block	☐ Allow writing
Smart phone	Write block / Block reading	☐ Allow writing / ☐ Allow reading
Tethering	Write block	☐ Allow writing
Modem	Write block	☐ Allow writing
Data cable	Write block	☐ Allow writing

[Device Control Policies]



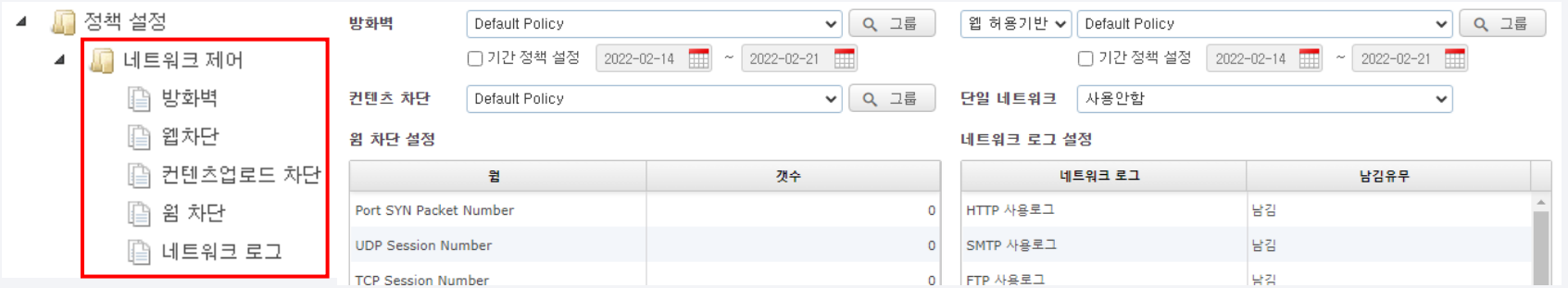
[Smartphone Block Message]

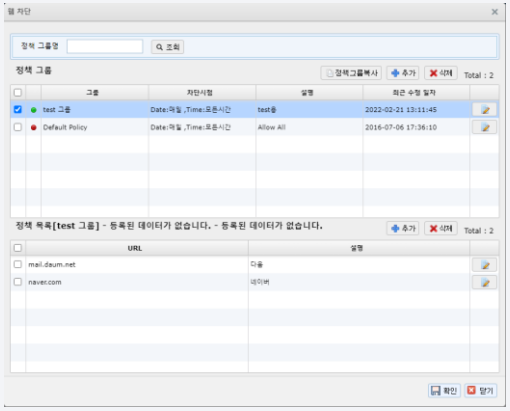


[USB Block Message]

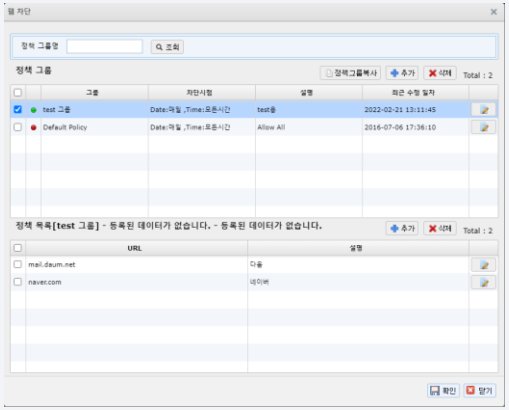
- Control and log the Read/Write of secondary memory media (floppy, CD/DVD, USB, external hard drive, smartphone MTP/PTP communication, etc.)
- Control the Allow/Block of wireless networks (Wi-Fi, Bluetooth, Wibro, tethering, etc.)
- Allow access only to wireless APs specified by the administrator (registered SSID control)
- If the 'Portable Storage Device' policy is blocked, general storage devices(USB, external HDD, etc.) can be registered and used as an exception.

III. Main Features – Network Control

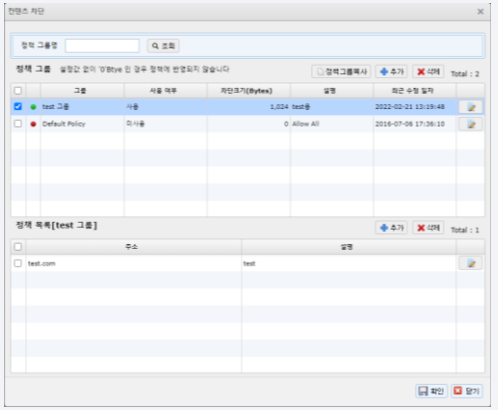




[URL Block Policies]



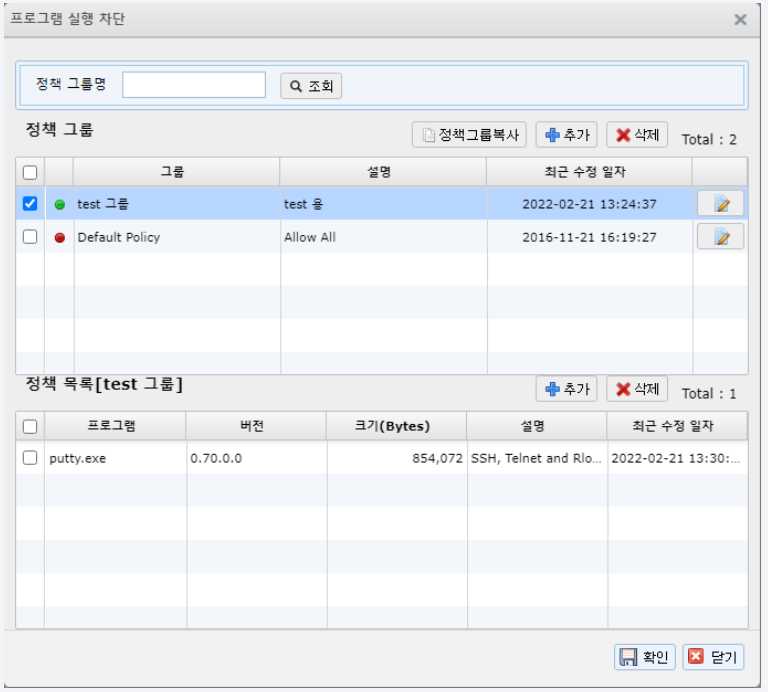
[Firewall Policies]



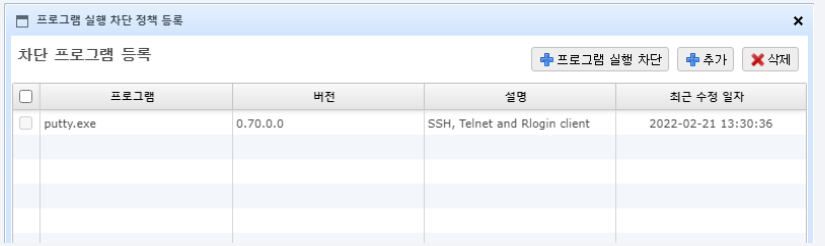
[Content Upload Block Policies]

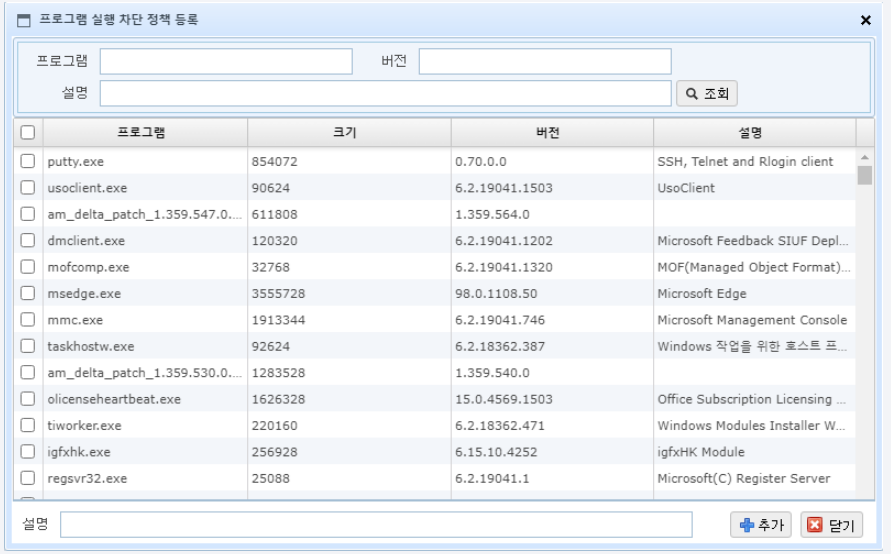
- Block access to web pages (blacklisting, whitelisting)
- Personal firewall (control by port, protocol, IP)
- Block attachment uploads such as webmail (control by specifying the size of attachments)
- Single network card setting (select the network card to be used by the user when applied)

III. Main Features – PC Security Settings(1/2)



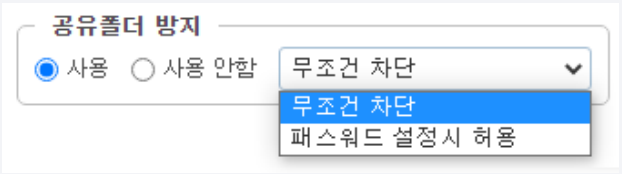
[Program Execution Prevention Policies]



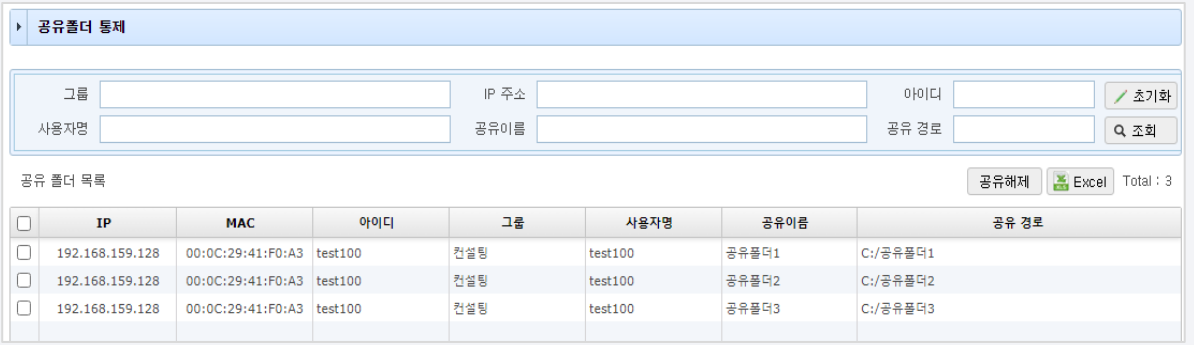


- Registering programs to prevent them from running
- Hash of the file is registered, so it can be blocked even if the file name is changed
- Provide the feature to register programs on the Agent PC (collect asset status on the PC)
- Even if the program on the program execution blocking registration list is not installed, it can be loaded after installing the program to be blocked on the console-connected PC.

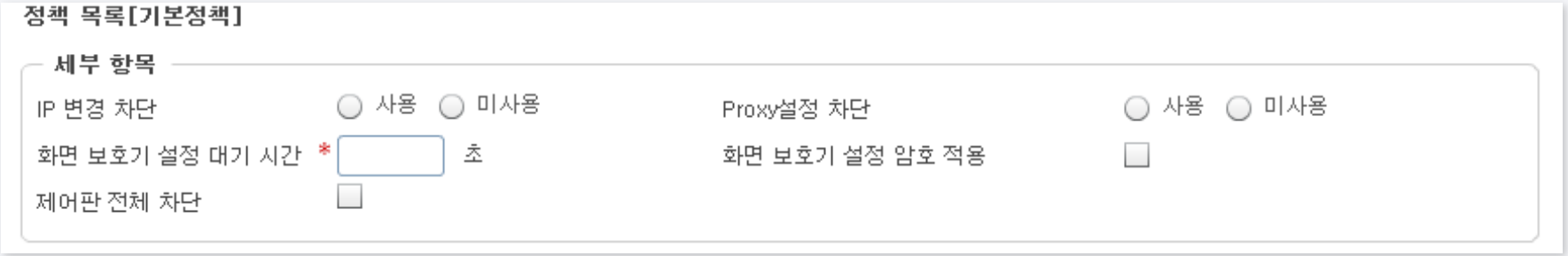
III. Main Features – PC Security Settings(2/2)



[Shared Folders Policies]



[Shared Folders Status]



[Other PC security Policies]

- View shared folders set up on Agent PCs and prevent them from being turned off or created
- Set Windows password complexity and prompt users to set a password if one is not set
- Force a screensaver and pop up a password prompt when the screensaver is turned off

III. Main Features – Process of Privacy Policy

MarkAny

Patterns

Setting up regular expressions, keyword patterns

Ratings

Setting up leakage control policies

Create policies

Combining patterns and Ratings

Apply policies

Policies by departments, users

Index

Scanning all files on the PC

Leakage control

Controlling leakage through devices, networks, and prints

Regular expression patterns

Patterns

Provide check expressions to search for strings with specific rules (13 default regular expressions are provided, such as social security numbers, passport numbers, etc.)

Leakage Control Policies

Ratings

Set policies to control the leakage of detected personal information files via portable storage devices, networks (such as mail), printouts, etc.

Keyword patterns

Patterns

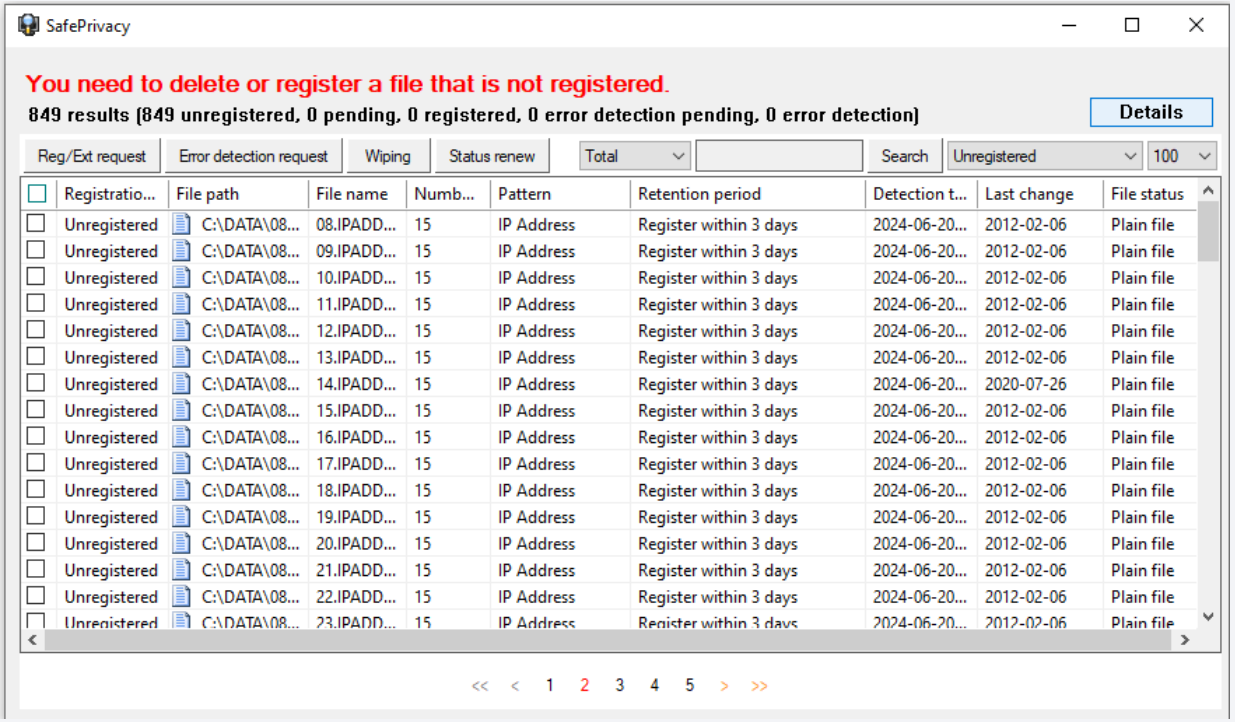
Allows administrators to add the ability to search for specific text within a document in addition to regular expression patterns (private, secret, confidential, etc.)

Optional Policies

Apply policies

Set up leak control policies for undetectable files, file register policies, how often to receive logs and policies, etc.

III. Main Features – Privacy detection status



[Privacy Detection Result (User)]

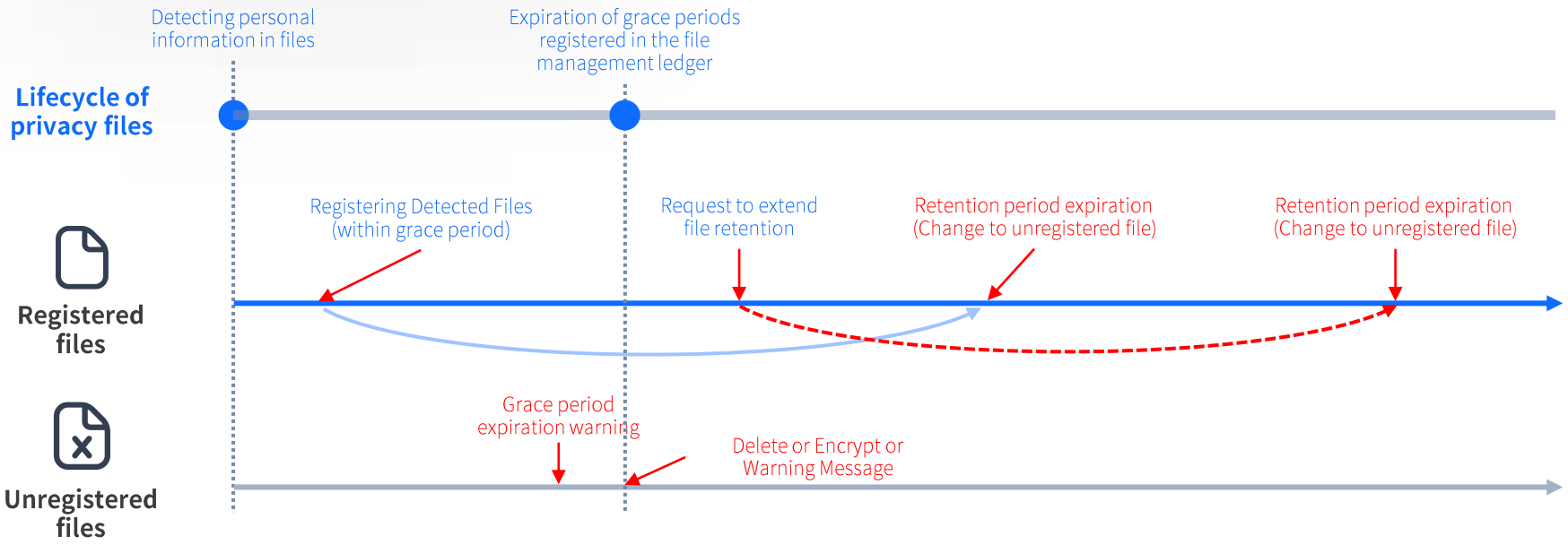
- Users can view the results of privacy (important information) detection according to the policy through the tray menu (double-click to view detailed status)
- The detected file is available after registration, and when the usage period expires, it is used after applying for an extension (File Management Ledger)
- Administrators can view the detection history of each user in the web console.

III. Main Features – File Management Ledger

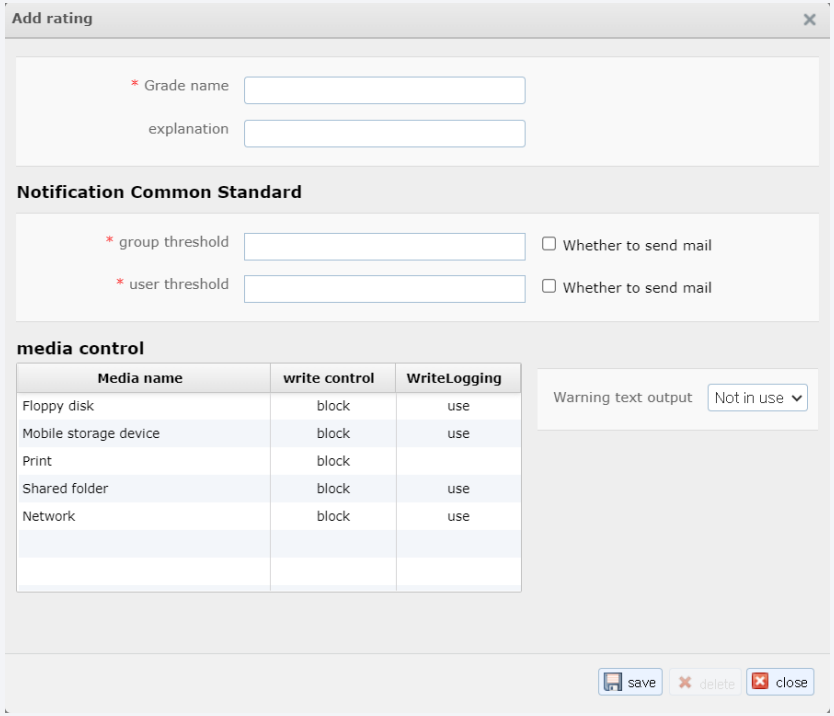
- Operation of the File Management Ledger in accordance with the Personal Information Protection Act “Article 32 Registration and Disclosure of Personal Information Files”, the Enforcement Rules “Article 3 Form of Books and Documents Related to Personal Information Protection Business”, and the Electronic Financial Supervision Regulations “Article 13 Computerized Data Protection Measures”.

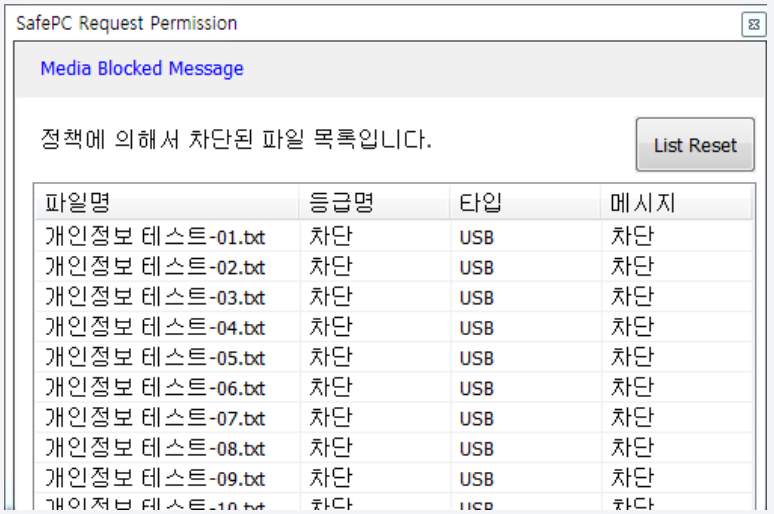
- The File Management Ledger is a method of registering and managing privacy files held by users. It provides safe management of personal information files by explaining the purpose and laws for retaining such files and deleting them completely when the retention period has expired.

Lifecycle of the File Management Ledger



III. Main Features – Control of Privacy Leaks

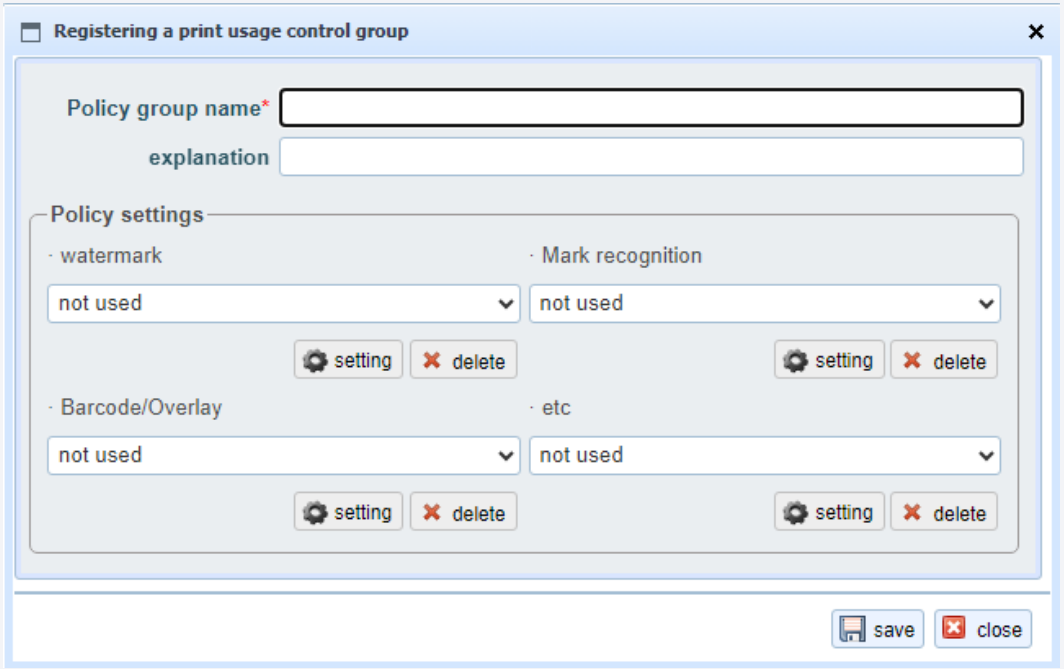




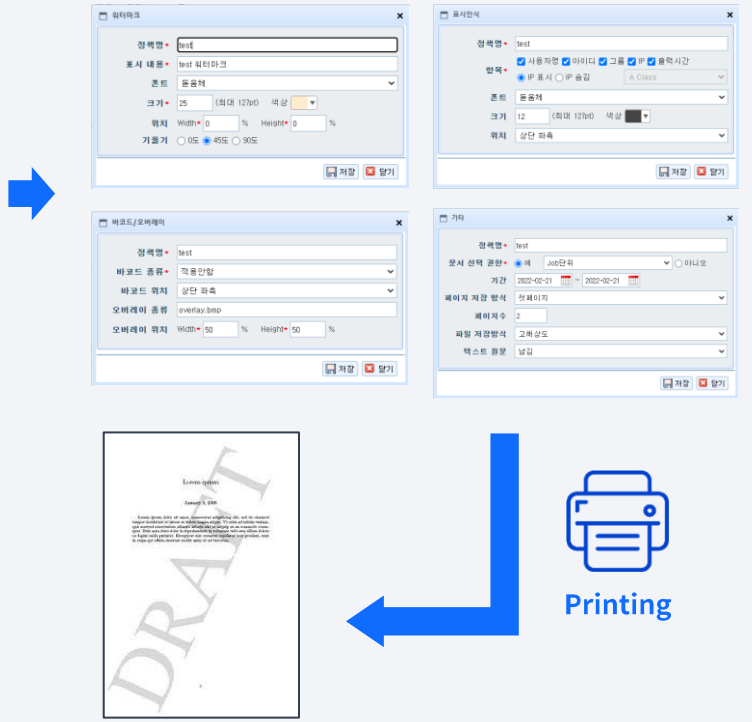
[Privacy Block pop-up]

- Controls leakage of detected personal information files to storage devices / prints / shared folders / networks (Features of Allows/Blocks, Write logging, and Save original text)
- In case of network, only analyzed protocols are supported
  - Website: Naver, Daum, Nate, DreamWiz, Clairvoyant, Korea.com, Google, JoinsMSN, Facebook, Whatsapp, Twitter
  - Messenger: (File attachment control) Nate-on, MSN, YAHOO, Mitsuri, Taki, POP Messenger / (Drag&Drop control) Line, Skype, KakaoTalk, FreeBond
  - Others: Outlook, SMTP (25port)

III. Main Features – Print Control

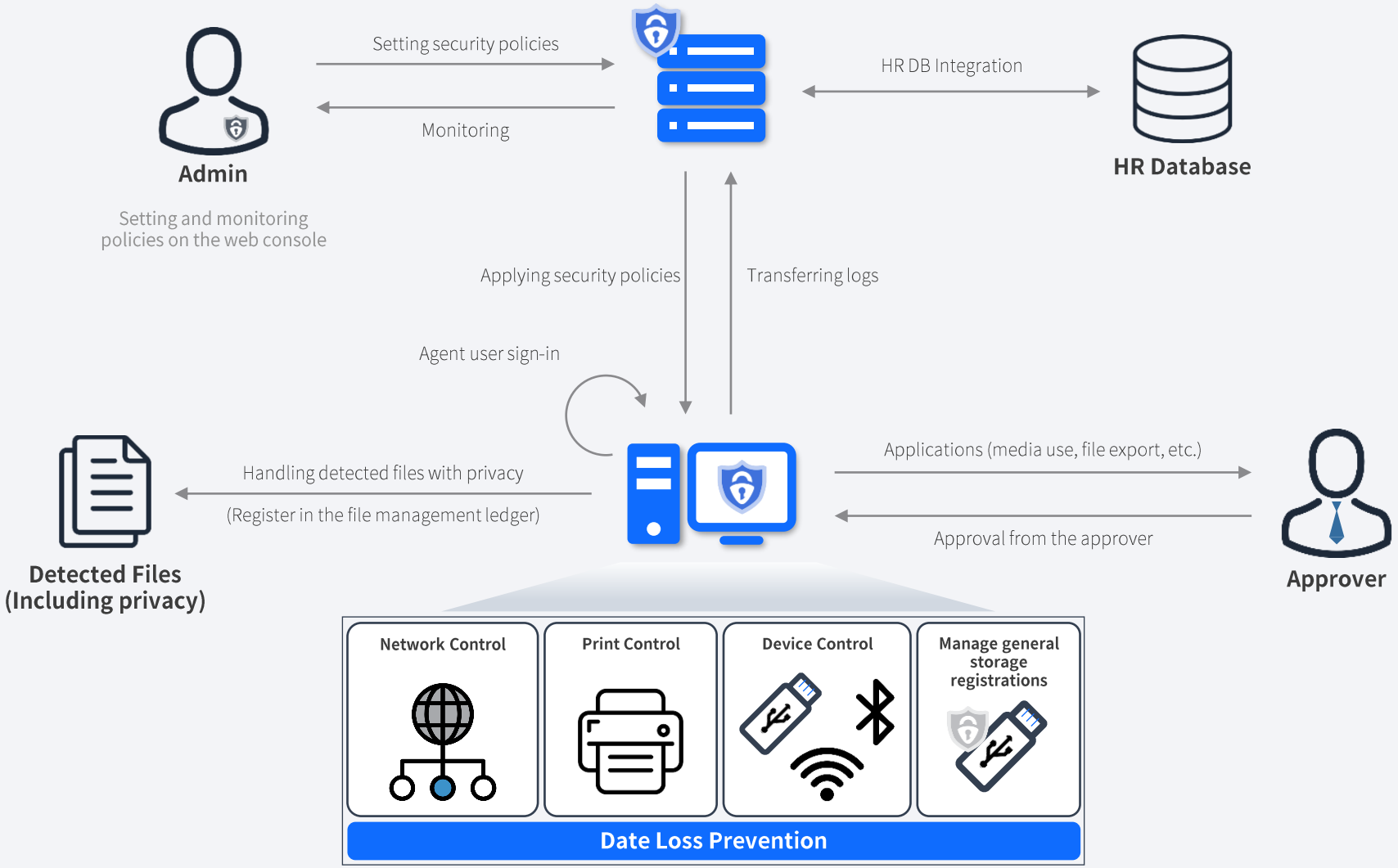


[Print control Policies]



- Block/Allow Policies of Printing
- Provide image/text watermark when allowing print (adjustable position)
- Print out printer information (username, ID, department, IP, print time, etc.)
- Save printing logs and copies

III. Main Features – Operation Process



III. Main Features – Approval Process

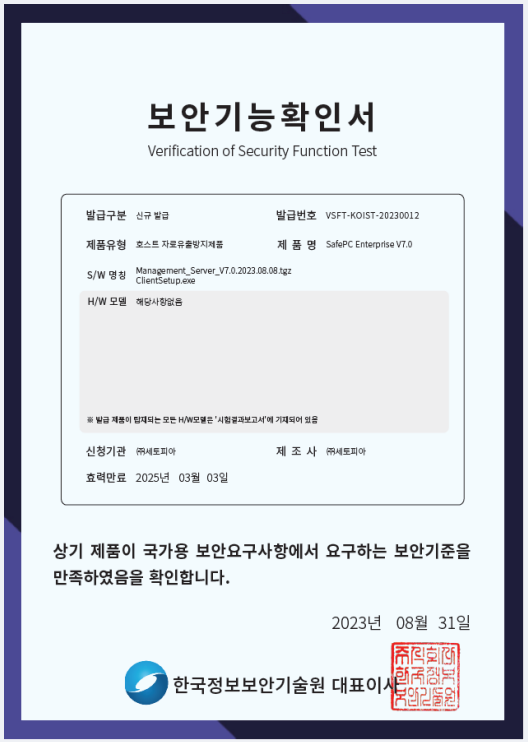
Category	Approval Process	내용
Common	Apply for user registration	• If you want to enroll additional users beyond the associated user, you can apply for them from the Application • Administrators can also add them from the console
	Apply to use Device	• Request an Exception to Device Control policies • Select internal/external, duration, device, and more to request an exception.
	Apply to register General Storage Device	• Allow registered general storage device even if device control policy is “Block” • Plug-in the device and extract the serial number to register it with the server • Exception is available only when the registered device is in internal state (can communicate with the server)
	Apply to accept Bad USB	• BadUSB: Manipulates the firmware of a regular USB to recognize it as a keyboard or mouse and execute malicious code (exploits the fact that the human interface is excepted in DLP systems) • Block all unregistered devices, including keyboards and mouse (whitelisting method)
DLP	File Export Request (General/Large size)	• File-by-file request for exceptions with blocking policy applied • To apply for exporting, users upload files and specifies file PW (download encrypted ZIP file after approval)
	Apply for registration in the File Management Ledger	• If you need to use the detected personal information file, register in the ledger to use it according to the privacy policy • Enter the purpose and period of retention, get authorization from the approver, and use it for that period of time • If you need to extend the period of use, apply for an extension and use it
	Request false positive/ false negative files	• Files detected by the Privacy Policy, but may be false positives or false negatives • Users can apply for an exception to the Privacy Policy if they believe a file is a false positive or false negative • Even if the file is registered as a false positive, if the file is modified and saved, it will be treated as a personal information file again
	Request to print official documents	• The printout is watermarked by the printing security policy • If you need it with watermark removed, apply for the exeption
	Request a printout	• Request to print if it is blocked by privacy policy • Upload the file you want to print and apply for printing, and select whether to exclude masking.

IV. Certification

SafePC Enterprise V7.0 has acquired ‘Verification of Security Function Test' and 'GS Certification’, and is on the Digital mall of the Public Procurement Service

SafePC Enterprise V7.0

- Verification of Security Function Test
  : August, 2023



보안기능확인서

Verification of Security Function Test

발급구분	신규 발급	발급번호	VSFT-KOIST-20230012
제품유형	호스트 자료유출방지제품	제 품 명	SafePC Enterprise V7.0
S/W 명칭	Management_Server_V7.0.2023.08.08.tgz ClientSetup.exe		
H/W 모델	해당사항없음		

※ 발급 제품이 탑재되는 모든 H/W모델은 '시험결과보고서'에 기재되어 있음

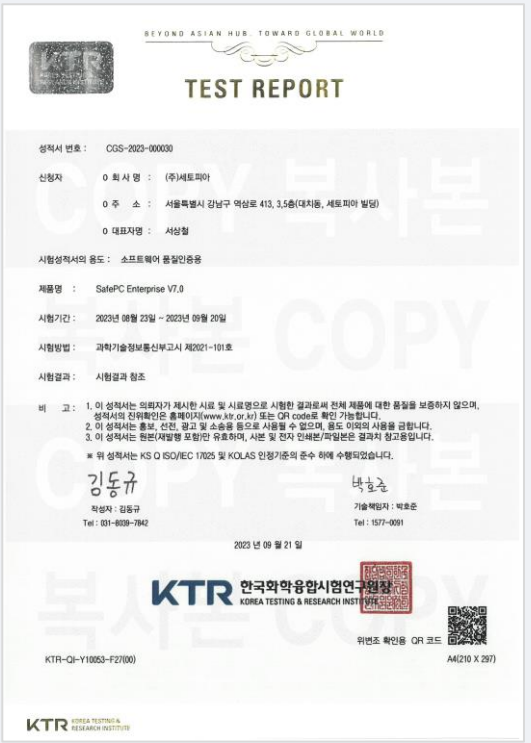
신청기관	㈜세토피아	제 조 사	㈜세토피아
효력만료	2025년 03월 03일		

상기 제품이 국가용 보안요구사항에서 요구하는 보안기준을 만족하였음을 확인합니다.

2023년 08월 31일

한국정보보안기술원 대표이사

- GS Certification : September, 2023



BEYOND ASIAN HUB TOWARD GLOBAL WORLD

TEST REPORT

성적서 번호 : CGS-2023-000030

신청자 ㅇ 회 사 명 : (주)세토피아

ㅇ 주 소 : 서울특별시 강남구 역삼로 413, 3,5층(대치동, 세토피아 빌딩)

ㅇ 대표자명 : 서상철

시험성적서의 용도 : 소프트웨어 품질인증용

제품명 : SafePC Enterprise V7.0

시험기간 : 2023년 08월 23일 ~ 2023년 09월 20일

시험방법 : 과학기술정보통신부고시 제2021-101호

시험결과 : 시험결과 참조

비 고 : 1. 이 성적서는 의뢰자가 제시한 시료 및 시료명으로 시험한 결과로써 전체 제품에 대한 품질을 보증하지 않으며, 성적서의 진위확인은 홈페이지(www.ktr.or.kr) 또는 QR code로 확인 가능합니다.
2. 이 성적서는 홍보, 선전, 광고 및 소송용 등으로 사용될 수 없으며, 용도 이외의 사용을 금합니다.
3. 이 성적서는 원본(재발행 포함)만 유효하며, 시본 및 전자 인쇄본/파일본은 결과치 참고용입니다.

※ 위 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정기준의 준수 하에 수행되었습니다.

작성자 : 김동규 Tel : 031-8039-7842

기술책임자 : 박호준 Tel : 1577-0091

2023 년 09 월 21 일

KTR 한국화학융합시험연구원장 KOREA TESTING & RESEARCH INSTITUTE

위변조 확인용 QR 코드

KTR-QI-Y10053-F27(00) A4(210 X 297)

KTR KOREA TESTING & RESEARCH INSTITUTE

SAFE PC ENTERPRISE

THANK YOU

MarkAny